CHECKLIST FOR COMPLIANCE WITH MONEY LAUNDERING REGULATIONS 2017 ('MLR17')

Contents

1. Anti-Money Laundering ('AML') & Terrorist Financing ('TF') Compliance Checklist

This checklist has been issued to assist IPA members with your work in remaining in compliance with the MLR17. It may assist with considerations as to your current internal practices and policies and reviewing these to ensure that your practices and policies are robust.

Please also continue to consult with any outside compliance agents that you work with and it is important that all practices, policies and procedures are reviewed and discussed internally – and where appropriate are approved by the Board/Senior Management.

This checklist is designed to assist you with your work regarding Money Laundering risks and considerations in respect of insolvency work. It is not formal regulation and you should continue to review and consider matters with your Money Laundering Reporting Officer ('MLRO'))/Money Laundering Compliance Officer ('MLCO'), your compliance officers/agents and team members to ensure that your policies and procedures deal with the risks from Money Laundering and Terrorist Financing that you have identified in your firms risk assessment.

As this is not formal regulation and is not subject to agreement with the other RPBs, this guidance, whilst designed to assist members with consideration as to the risks and issues that arise from MLR17, should not be treated as such formal regulation/legal guidance or advice.

If general advice and assistance on AML matters is required, please remember that the IPA have a general helpline email at – amlhelpline@ipa.uk.com

2. FIRM RISK ASSESSMENT – Regulation 18

You must take steps to identify and assess the risks of money laundering to which your firm may be subject. The details completed below will provide an overview of your firm which you should then utilise to assist with completion of your risk assessment.

You should consider each 'type' of appointment taken and the risks associated with the different appointments to highlight where an appointment may have a higher risk of money laundering. For example, if you carry out corporate work only, do you consider that MVL cases have a higher risk than CVL cases?

You should also consider the risk element for each part of the assessment and grade as 'High' or 'Low' risk. Members should note in the risk assessment the greater risk where contact and work is carried out on-line, which can raise the risk of your services being used for money laundering. Members should also consider the risks where an appointment commences with direct contact from the directors and ensure that suitable checks are made regarding identity.

Geographic checks should consider cases that are offered to you, or contact made directly, where the business traded, or the individual is resident in a different part of the UK to you/your office(s).

Matters to consider which may indicate a higher risk for your business include:

- undue client secrecy (e.g., reluctance to provide requested information and which may be heightened due to on-line contact);
- unnecessarily complex ownership structures;
- do you deal with any of the following business activities:
  - cash-based businesses – i.e. take-away business, restaurants etc.
  - money service bureaus
  - property transactions with unclear source of funds or where there are a number of large transactions
  - nail bars/salons
  - business that supply temporary workers
- rapid close down – where a company is set-up either off-shelf or after a buy-out of assets from a prior CVL, trades for a short period running up dents (especially large HMRC debts) and then closes down as insolvent
- work outside its normal range of goods and services;
- the source of funds is unusual or unknown;
- high net worth individuals;

- uncooperative clients;
- transactions are inconsistent with known business and personal information;
- multiple bank accounts, foreign accounts with no good reason, online banking not hosted in the UK; or
- altering professional advisors a number of times in a short space of time without legitimate reasons,
- the service being requested was refused by another professional advisor without legitimate reasons

You should also be aware of Reg 18(4) and keep an up-to-date record, in writing, of all the steps taken to identify and consider the risks of money laundering to which your business is subject. These records are able to be reviewed as part of any inspection visit or compliance review.

Name of Organisation:	
Licensed IPs and RPBs:	
Number of staff:	
Number of premises:	
Approximate number of ongoing assignments:	
Approximate number of new assignments p.a.:	
Value of transactions:	
Turnover:	
Main services provided (i.e. insolvency only, or also turnaround, business rescue etc.):	1.
	2.
	3.
Main areas of insolvency dealt with (i.e. MVL/CVL/IVA etc.):	1.
	2.
	3.
Any specific industries or type of client your organisation deals with?	1.
	2.
	3.
Any other specific areas or issues in respect of assignments/appointments/work carried out? Consider: • Client risk • Country/geographic risk • Product/Service risk	

• Transaction risk • Delivery Channel risk	

If you do not have a risk assessment for your organisation, you are in breach of Regulation 18 of MLR17. Please remember that your Supervisory Authority can request a copy of your organisations risk assessment at any time and they could potentially carry out a targeted visit to review all your AML/TF policies and procedures and/or (depending on the Supervisory Authorities internal rules) commence regulatory action for a breach of MLR17.

3. POLICIES – REGULATION 19

As well as having a current and up-to-date risk assessment for your organization, you should also have in place formal policies, which are proportionate to the size and nature of your organisation).

The following areas should be considered as to whether you have, or require a formal policy (please note that this is not prescriptive and your organisation should consider policies that deal with matters that affect your business):

Policy Area	**Mark if policy in place?**	
AML policy	Yes	No
Risk Management	Yes	No
Internal Controls	Yes	No
CDD policy	Yes	No
Reporting & Record-Keeping	Yes	No
Suspicious Activity Reports ('SARs')/disclosures to National Crime Agency ('NCA')	Yes	No
Monitoring, communicating & managing compliance with internal policies	Yes	No
Identification and Enhanced Due Diligence ('EDD') for large, complex & high-risk areas of work	Yes	No
Whistleblowing policy	Yes	No

For any where you have highlighted 'no' – it is recommended that you should consider drafting a policy to deal with that area. All are areas that appear in MLR17 and the IPA would expect some internal guidance or procedure to be in place that ensures all staff are aware of what is expected of them in relation to these areas.

The IPA would recommend that staff are asked to confirm their understanding of what is required from them in relation to a particular policy. If they are not able to explain what is needed from them, the policy should be reviewed to ensure that it is clear and effective.

When considering drafting a policy, it should consider the following areas to make your policy as robust as possible:

	Mark when considered
Size of your organization and nature of business	
Will the policy be part of a manual, handbook or a single page statement?	
Does any policy require board/senior management approval?	
When will policies be reviewed and updated?	
Will you need to draft or include a form for staff to use (i.e. a Politically Exposed Person ('PEP') form, or SARs notification form)?	
How will new and updated policies be communicated to staff?	

4. CONTROLS – REGULATION 21

It is a requirement under MLR17 that any organisation has controls in place in relation to money laundering and terrorist financing procedures and policies so that they are subject to review and testing for their effectiveness and robustness.

The following areas should be considered for controls (again these will need to be proportionate to the size of your organisation):

	Mark when considered
Risk management profile review	
Has the NO been appointed and do they have sufficient seniority and knowledge of ML/TF issues?	
Does and has a Money Laundering Compliance Officer ('MLCO') been appointed?	
Are there regular reports (these should be at least annually) to the Board/Senior	

Management on AML/TF issues and do the Board/Senior Management approve all new, updated policies and procedures?	
Does your audit check, review and test the efficacy and robustness of policies and procedures? An audit can be carried out internally or by a compliance agent/third party	
How do you assess that your employees have the necessary skills, knowledge and expertise to carry out their functions in indentifying and mitigating the risks of AML/TF? This assessment needs to be undertaken before and during employment	
How will AML/TF issues be communicated to the staff and how will compliance be monitored?	
How will new members of staff be trained/introduced to the organisations AML/TF culture?	
Does the Board/Senior Management team look to promote and embed a culture of AML/TF compliance in the organisation?	

5. RECORD KEEPING – REGULATION 40

One of the important areas of MLR17 is the need for any organisation to keep records of AML/TF matters.

1. The following are areas that it is recommended that formal records are in place and this should be considered to be included as either a stand-alone policy on record-keeping and/or included in relevant internal policies and procedures. These records can form the basis of a defence against accusations of failing to carry out duties under POCA and the 2017 Regulations. Businesses should consider their retention policies taking into account both data protection and the potential for law enforcement contact:

Information	**Mark if in place**
Appointment of the NO and MLCO (as appropriate) – including notification of identity to your Supervisory Authority and how their identity(ies) are communicated to all staff	
PEP forms	
Training Records and Training Log – including evidence of how new and updated	

policies are communicated to all staff	
Annual and other reports to senior management	
SARS lodged	
Cases/assignments where you had to terminate the engagement due to not beings supplied or provided with appropriate initial due diligence information to verify identity	

2. The following records should be retained for a period of **5 years** after the end of a business relationship (or an occasional transaction that is not carried out as part of a business relationship):

Information	**Held?**
Copies of the evidence obtained to verify the client's identity (personal and corporate where required)	
Information on the purpose and nature of the business relationship/work to be carried out	
Information obtained on the transactions/activity subject to CDD (including ongoing monitoring)	
Full details of **internal** and **external** suspicious activity reports (SARs) and actions taken in respect of these (this includes information considered by the NO, the justification as to why an external SAR was or was not made, and communications with the National Crime Agency) – the MLRO query log	
If you keep any additional records, please specify these:	

6. REPORTING PROCEDURES & TIPPING-OFF

A policy should be on place and circulated to all staff in your organisation that advises what they should do if they form the suspicion of money laundering by a client or third party and how this is discussed with your NO and a submission made to the NCA if it is considered that the a SAR needs to be submitted.

The policy should also include a reminder about 'tipping-off' as well as a reminder that work on that area of an assignment or piece of work for which a submission to the NCA has been made cannot be proceeded with until the NCA have either provided consent or not responded to a Defence Against Money Laundering SAR ('DAML SAR') within 7 working days, A copy of your internal SARS form should be available for staff use.

The policy should also include reference to the recent dispensation from the NCA to IPs where for urgent issues an 'emergency DAML request' can be made. The request is only for those cases such as where an emergency/hostile appointment is made and funds are to be received where there is a suspicion the funds made be tainted. The request can cover urgent payments required from such funds (i.e. wages for trading Administrations).

It is also recommended that submissions of SARS are held on a secure database with access limited to the NO and MLCO (where appointed). As part of your SARS policy and/or information you provide to your staff you may wish to consider the following matters:

Are employees aware of the following?	**Mark when included**
What must be reported	
The failure to report an offence	
What is tipping-off	
Prejudicing and investigation offence	
When and how an external SAR is made to the NCA	
What is a DAML and why it is important	
What should happen after an external SAR is made	
Emergency DAML requests	

7. CDD

Due diligence work is required to be carried out before the establishment of a business relationship. Simple provision of advice where there is no engagement requested would not ordinarily be a business relationship.

However, should the advice result in a request to undertake insolvency or associated work a business relationship will need to be established and due diligence work must be undertaken. The Insolvency Appendix to the CCAB guidance on AML matters will assist IPs with the requirement.

Consideration should be made as to whether you request due diligence details as part of the letter of engagement, or prior to commencing work to confirm an appointment by deemed consent or via a decision procedure.

It is recommended that whatever policy is used, that the letter of engagement is clear that you will not accept funds, hold or deal with assets, or progress the matter to a formal appointment until due diligence work is completed.

1. Do you include matters relating to AML in your Letters of Engagement? For example:

	Included?
A description/full scope of work/services to be provided	
Your AML/TF obligations (including identity information the client	

must provide to you)	
Data protection information (noting that under Reg 40 of the MLR17 records should be retained for 5 years from when the business relationship or transaction has concluded. However, Reg 40(5)(a) indicates that GDPR regulations can apply and records can be held for six years.)	
That no work will be undertaken, assets or funds held or dealt with until the required detail and information to enable due diligence to be completed is provided and reviewed	

2. Is there a formal client risk assessment procedure for obtaining information on the business relationship and assessing the level of risk? Does it request and/or consider the following:

	Included?
Obtaining of identification documentation and verifying documentation?	
If electronic means are used to verify, have you informed the proposed client that such checks are to be carried out or obtained permission to do so by the proposed client?	
Issues arising from the identification and verification of identity of the client?	
For corporate clients – identifying and verifying the company and the beneficial owner and the persons of significant control ('PSC')?	
Where there is a discrepancy in the PSC – ensuring Companies House are notified	
Issues arising from the identification and verification of identity of beneficial owners?	
Checks on the 'wealth' of the entity? i.e. do you understand where funds originated and/or where asset purchases arose?	
When EDD is required?	
What further checks are required for EDD? (for example – do you check the F-ATF list of countries with unsatisfactory controls etc.)	
How checks are performed for PEPs and EDD carried out if a client is a PEP?	
The intended nature and purpose of the work to be carried out, including:	
- Client risk factors (including the client's source of money/assets, area of business etc.)	

- Product/Services risk	
- Geographical risk factors	
- Delivery Channel risk	
- Transaction risk	
- Has there only been contact on-line with the debtor or director and how you confirm identity	
What should happen if CDD is not able to be completed prior to an appointment/assignment under Reg 30 of MLR17?	
Termination of an appointment/assignment if CDD/EDD cannot be completed in a timely manner?	
How ML/TF matters on a case are to be subject to review during the life of the assignment?	

8. ASSET SALES

Does your policy include details on what CDD or EDD is required if asset sales or payments are received from a third party? Consider the following points:

	Included?
CDD on the identity of the payer/source of funds?	
In bankruptcy appointments if a sum of over €15,000 is to be paid – CDD on the purchaser must be undertaken. You should consider on a risk basis whether CDD is required on purchasers of assets for a sum of over €15,000 is required but this is not routinely required	
If the details obtained from the CDD checks raises questions and the assessment of the risk in respect of an asset sale indicates a higher potential risk – what EDD would be requested on the payer/funds?	
Is the sum to be paid over €10,000 in cash? If so, what procedure is in place to report to HMRC as a high value dealer?	

Date: Jan 2022
Review – Jan 2023